Terminal B includes a decoding device **14B** which corresponds to the decoding device **14** in the FIG. **2** configuration and which transforms received signed ciphertext word C_{As} to the signed message word M_{As} using terminal B's decoding key D_B. In addition, terminal B includes an encoding device **42B** which is similar in form to the encoding device **12A**, but which utilizes the signed message word M_{AS} as its data input and the encoding key E_A associated with terminal A as the key for that device **42B**. Device **42B** transforms the signed message word M_{As} to the unsigned message word M_A', which corresponds to the original message M_A. Thus, all of the devices **12A**, **14B**, **40A**, and **42B** are substantially the same in function but they utilize the indicated encoding or decoding keys and data inputs.

In alternative embodiments, the order of the enciphering and signing operations may be switched, provided that the order of the corresponding deciphering and unsigning operations are similarly switched. Furthermore, additional levels of enciphering or signing may also be utilized so long as there is a corresponding deciphering or unsigning operation.

While the system in FIG. **5** is suitable for signal direction transmission of a message from terminal A to terminal B, terminal B may also include blocks corresponding to blocks **12A** and **40A** and terminal A may include blocks corresponding to blocks **14B** and **42B** with the respective keys E_A, D_B, D_A and E_B, as shown in FIG. **6**. With the latter system, two-way signed digital communications may be accomplished. In alternative configurations, additional terminals may be utilized using the addition of similar blocks coupled to the channel **10**, with the appropriate keys and modem and addressing networks.

The signature systems described above in conjunction with FIGS. **2**, **4**, **5**, and **6** are suitable where the respective message and ciphertext words represent numbers less than the n_i for the particular transformations. As noted above, when the words to be transformed (either by encoding or decoding) are initially beyond the nominal range requirement, a blocking subsystem is used to break the word into blocks within that range before the transformation is performed. A corresponding unblocking subsystem is utilized following the inverse transformation at the receiving terminal to obtain the original message. FIG. **7** shows an exemplary configuration which is similar to the configuration of FIG. **5**, but which also includes blocking and unblocking subsystems. Terminal A of the configuration of FIG. **7** includes a first blocking subsystem **61** which precodes the message to a blocked message M_A, which in turn is transformed by device **40A** to a signed message M_{As}. A second blocking subsystem **63** transforms M_{As} to blocks M_{As}'' each block of which is then transformed by device **12A** to a signed ciphertext word C_{As}. At terminal B, C_{As} is first transformed to signed message blocks M_{As}'' by device **14B**, which are then transformed by a first unblocking subsystem **65** to the signed message word M_{As}. The word M_{As} is then transformed by device **42B** to the blocked message M_A, which is in turn transformed by a second unblocking subsystem **67** to the original message. In embodiments where the message is enciphered before signing, the device that first provides C_A which is transformed to C_A'' and then to C_{As}. At the receiving terminal C_{As} is first transformed to C_A'' which is then transformed to C_A and then decoded to M_A.

The blocking and unblocking subsystems may be configured with any of the various forms of the present invention wherein the respective message and ciphertext words are outside the nominal ranges. Where the range requirements for a word transformation are met, the blocking and unblocking subsystems are not utilized.

The encoding operation for the present invention will now be illustrated for the case where $p=47$, $q=59$, $n=p\cdot q=47\cdot 59=2773$, $d=157$ and $e=17$, to encode the message:

ITS ALL GREEK TO ME

Initially, the message is encoded with two English letters in a block, by substituting for each letter a two-digit number: blank=00, A=01, B=02, . . . , Z=26. In this form, the message is precoded to:

$$M=0920190001121200071805051100201500130500$$

Since this value for M is greater than n(=2773), M is broken into blocks $M_1, \ldots, M_{10}$ as follows:

$$M = M_1\ M_2\ M_3\ M_4\ M_5\ M_6\ M_7\ M_8\ M_9\ M_{10}$$
$$= 0920\ 1900\ 0112\ 1200\ 0718\ 0505\ 1100\ 2015\ 0013\ 0500$$

Since e=10001 in binary, the first block ($M_1=0920$) is enciphered using the encoding key E=(17,2773) to a corresponding ciphertext block C_1:

$$C_1 \equiv M_1^e \pmod{n}$$
$$\equiv M_1^{17} \pmod{2773}$$
$$\equiv ((((1)^2\cdot M)^2)^2)^2)^2)\cdot M \pmod{2773}$$
$$\equiv 948 \pmod{2773}$$

The whole message is enciphered as:

$$C = C_1\ C_2\ C_3\ C_4\ C_5\ C_6\ C_7\ C_8\ C_9\ C_{10}$$
$$= 0948\ 2342\ 1084\ 1444\ 2663\ 2390\ 0778\ 0774\ 0219\ 1655$$

The ciphertext can be deciphered in a similar manner using the decoding key D=(157, 2773). For the first block C_1:

$$M'_1 \equiv C_1^d \pmod{n}$$
$$\equiv 948^{157} \pmod{2773}$$
$$\equiv 920 \pmod{2773}$$

The other blocks are similarly deciphered so that the various blocks may be put together to form M, and then be decoded (by reversing the letter-to-two-digit-number transformation) to the original message.

In a public key cryptosystem utilizing the present invention, each user has an associated encryption key E=(e,n) and decryption key D=(d,n), wherein the encryption keys for all users are available in a public file, while the decryption keys for the users are only known to the respective users.

In order to maintain a high level of security in such systems, a user's decoding key is not determinable in a practical manner from that user's encoding key. Since